Hypothesis Test:

arxiv - 1704.01998

Numerical Simulation:

arxiv - 1803.04167

Me:

danmills0.github.io

Further Reading

Blind Quantum Computing:

Fitzsimons, Joseph F. - “Private quantum computation: an introduction to blind quantum computing and related protocols.”

Verification:

Gheorghiu, Alexandru, Theodoros Kapourniotis, and Elham Kashefi. - “Verification of quantum computation: An overview of existing approaches.”

Mahadev, Urmila. - “Classical Verification of Quantum Computations.”

IQP:

Shepherd, Dan, and Michael J. Bremner. - “Temporally unstructured quantum computation.”

Bremner, Michael J., Richard Jozsa, and Dan J. Shepherd. - “Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy.”

Verification of Early Stage Quantum Computation

Daniel Mills - daniel.mills@ed.ac.uk
IF-5.19, School of Informatics, 10 Crichton Street, Edinburgh, EH8 9AB

Introduction

Quantum computers may revolutionise the technology industry. However:

I'm going to build a quantum computer.

Good luck, it's hard.

Okay, maybe one of the small ones which are easier to build.

You know, those ones that can do some but not all quantum computations.

If it is not very quantum how do you know it is not just classical?

Ummm...

Also these devices experience errors so the output might just be random noise.

Golly, I didn't think about these things.

We suggest:

- *IQP* as a small (*non-universal*) quantum computer to explore.
- A *Hypothesis test* to confirm some quantumness.
- *Numerical simulations* to judge the effect of noise.

Preliminaries

Qubits: Classically a bit can be in the state 1 or 0. Quantumly these states are represented by $|1\rangle$ and $|0\rangle$ which we call the *computational basis*. A quantum bit, or *qubit*, can also be in the 'half $|0\rangle$, half $|1\rangle$' *Hadamard basis*:

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \quad , \quad |-\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle . \tag{1}$$

Measurement: If we *measure* $|+\rangle$ *in the computational basis* we are equally likely to obtain $|0\rangle$ or $|1\rangle$. If we measure in the Hadamard basis we obtain $|+\rangle$ with certainty. More generally, if we have the state $|\psi\rangle = \alpha\,|a\rangle + \beta\,|b\rangle$, then, if we measure in the $\{|a\rangle\,, |b\rangle\}$ basis, we will obtain $|a\rangle$ and $|b\rangle$ with probabilities α^2 and β^2 respectively.

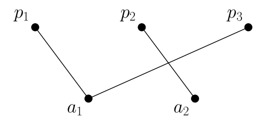
Entanglement: Given two states, $|+\rangle$ and $|0\rangle$, we can write the *composite system*:

$$|+\rangle \otimes |0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle . \tag{2}$$

We can *entangle* these states by applying a CNOT gate (acting on each binary string as if classical) to obtain $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. If one measures the first qubit, $|0\rangle$ is obtained with probability $\frac{1}{2}$. The state must then switch to $|00\rangle$ and you will measure the second qubit in the state $|0\rangle$. However, if you measure the second and not the first then you will obtain $|0\rangle$ with probability $\frac{1}{2}$. But how does the second qubit know if you have or have not measured the first?!? This is part of the power of quantum mechanics.

IQP

IQP is implemented by entangling $|+\rangle$ states according to edges of *IQP graphs*:



This entangled state is then measured to obtain a classical bit string as output.

Hypothesis Test

How are you going to check you have a quantum computer?

Unlike classical computers, quantum computers can factor large numbers.

That's the most famous application. If it can do that I'll know.

You need a universal machine for that.

Fine! How about I send a hypothesis test.

A *Hypothesis Test* allows a user to check a device has the power of IQP by:

- Solving a problem that is hard for a classical computer but easy quantumly.
- Allowing a classical user a means to check the solution.

Factoring does this (given factors, multiply together to check) but is too hard for an IQP machine. Instead, we use the *bias* of the output distribution in the direction s:

$$\text{Bias}\,(x,s) = \mathbb{P}\,(x \cdot s = 0) = \text{“}\textit{probability the output, } x\textit{, is orthogonal to } s\text{”}$$

I'll ask the device to implement an IQP graph depending on an s I know.

The bias is a function of s so I can check the outcome.

If the graph depends on s wouldn't a classical machine know s?

Then they can calculate the bias in the same way you did?

You're right, I need to hide the graph.

Blind quantum computing lets us remotely build a quantum state without revealing the state to the person building it. Hence the steps of our protocol are as follows:

1. Randomly generate s and calculate the bias to expect.
2. Ask the quantum device to blindly build and measure graph corresponding to s.
3. Compare the outputs bias in the direction s to your calculation.

Numerical Experiments

Building a quantum computer will be hard since qubits are noisy.

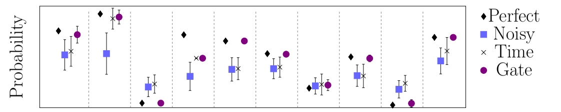
A noisy quantum computer is still a quantum computer.

Actually if it is too noisy the output might just be totally random.

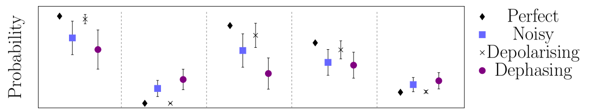
I could just as well produce random numbers with a classical computer.

Okay, let's numerically model the impact of different types of noise.

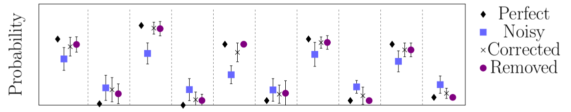
Only Gate Based Noise and Only Time Based Noise: We compare the impact of gate based noise (applying the wrong gate) and time based noise (decay of data over time). Notice that time based noise has the greatest impact.



Only Dephasing Noise and Only Depolarising Noise: We divided time based noise into depolarising (errors due to interaction with surroundings) and dephasing (errors due to the accuracy of measurement in some basis being better than others). The greatest deviation from perfect is caused by the dephasing error.



Error Corrected Dephasing: Finally we studied the impact that a simple error correction code would have on the noise. It would seem to be substantial and so we are optimistic that this could be a solution to the problem of noise.



Many thanks to my sponsors for supporting this work:

EPSRC Engineering and Physical Sciences Research Council
THE UNIVERSITY of EDINBURGH informatics
EPSRC Centre for Doctoral Training in Pervasive Parallelism

LaTeX TikZposter